Developing the Advanced Encryption Standard

Miles Smid and Ed Roback

National Institute of Standards and Technology
U.S. Department of Commerce

Outline of Presentation

- What has been done so far
- Candidate Algorithms and some of their properties
- Next Steps
- Request for Formal Comments
- Questions

AES Goal

- Selection of a standard that supports (at least) 128, 192 and 256 bit key sizes; block size of 128 bits
- Worldwide-royalty free
- More secure than Triple DES
- More efficient than Triple DES

What has been done so far?

- Announcement of intent to develop AES and request for comments, January 2, 1997
- Workshop on proposed requirements and procedures, summary of comments, April 15, 1997
- Informal draft requirements and procedures, June 16, 1997
- Formal call for candidate algorithms, Sep. 12, 1997
- Submission for pre-review, April 15, 1998
- Close of call, June 15, 1998
- Notification to submitters, July, 1998
- First AES Candidate Conference and beginning of Round 1 evaluation, August 20-22, 1998
- NIST to establish informal discussion group at www.nist.gov/aes for each candidate, Sept. 1998
- Formal FR call for public comments, Sept. 14, 1998

Selecting the Candidates

- Twenty-one packages received
- NIST verified that legal documents were completed
- NIST verified that responses were provided for all items
- NIST attempted to run code and verify Known Answer Tests
- Six packages found to be incomplete
- No cryptanalysis initially performed

Candidate Algorithms

- Australia
  - LOKI97 — Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
- Belgium
  - RIJNDAEL — Joan Daemen, Vincent Rijmen
- Canada
  - CAST-256 — Entrust Technologies, Inc.
  - DEAL — Outerbridge, Knudsen
- Costa Rica
  - FROG — TecApro Internacional S.A.
- France
  - DFC — Centre National pour la Recherche Scientifique (CNRS)
- Germany
  - MAGENTA — Deutsche Telekom AG

Candidate Algorithms, cont.

- Japan
  - E2 — Nippon Telegraph and Telephone Corporation (NTT)
- Korea
  - CRYPTON — Future Systems, Inc.
- USA
  - HPC — Rich Schroeppel
  - MARS — IBM
  - RC6 — RSA Laboratories
  - SAFER+ — Cylink Corporation
  - TWOFISH — Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
- UK, Israel, Norway
  - SERPENT — Ross Anderson, Eli Biham, Lars Knudsen

Related Presentations at this Conference

- The RC6 Block Cipher
  - Ron Rivest, RSA Laboratories
  - Tuesday, 2 PM, Cryptographer's Track
- MARS: IBM's AES Proposal
  - Dave Safford, IBM
  - Tuesday, 3 PM, Cryptographer's Track
- The Twofish Encryption Algorithm
  - Douglas Whiting, Hi/fn
  - Tuesday, 4 PM, Cryptographer's Track

Evaluation Criteria

- Security
  - Actual Security
  - Random permutation properties
  - Mathematical basis
  - Other security factors raised
- Cost
  - Computational efficiency
  - Memory requirements (hardware and software)

Criteria Continued

- Algorithm and Implementation Characteristics
  - Flexibility
  - Hardware and software suitability
  - Simplicity of design

Comments Requested

- How well algorithms meet criteria
- Any related intellectual property
- Cross-cutting analysis of multiple algorithms
- Overall recommendations and rationale

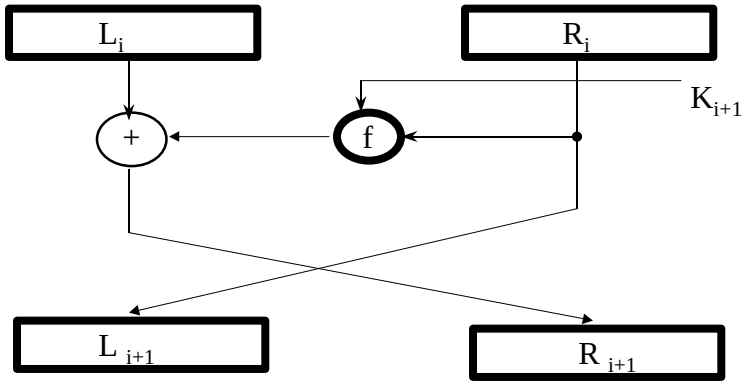
Security

- Based on Previous Schemes and Methods
- Cryptanalysis

Based on Previous Schemes

AES Candidate	Precursor(s)
• CAST-256	CAST-128
• DEAL	DEA
• LOKI97	LOKI 89,91
• RC6	RC5
• SAFER+	SAFER

Feistel Transform (Inversion)



+ = bitwise XOR

TWOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Feistel Networks (F)

Algorithm	Rounds
DEAL	6,6,8
DFC	8
E2	12
LOKI97	16
MAGENTA	6,6,8
TWOFISH	16

TWOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Modified Feistel Networks (MF)

Algorithm	Rounds	Cycles
CAST-256 (MF1)	48	12
MARS (MF3)	32	16
RC6 (MF2)	20	10

TWOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Substitution-Permutation Networks (SP)

Algorithm	Rounds
CRYPTON	12
Rijndael	10,12,14
SAFER+	8,12,16
SERPENT	32

TWOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Other Algorithms

Algorithm	Rounds	Type
FROG	8	Key Interp.
HPC	8	Omni

Cryptanalysis 1

- LOKI97
  - Rijmen and Knudsen
  - Differential: 2^{56} chosen plaintexts
  - Linear: 2^{56} known plaintexts
- FROG
  - Wagner, Ferguson, and Schneier
  - Differential: 2^{58} chosen plaintext
  - Linear: 2^{56} known plaintexts

Cryptanalysis 2

- MAGENTA
  - Biham, Biryukov, Ferguson, Knudsen, Schneier, Shamir
  - 2^{64} chosen plaintexts, 2^{64} steps
  - 2^{33} known plaintexts, 2^{97} steps
- DEAL
  - 2^{70} chosen ciphertexts, 2^{121} steps, (Lucks, 128)
  - 2^{70}, chosen plaintexts, 2^{121} steps, (Knudsen, 192)
  - 2^{56} chosen ciphertexts, 2^{145} steps, (Lucks, 192)
  - Meet in middle, 2^{224} steps, (Knudsen, 256)

Cryptanalysis 3

- SAFER +
  - 2 known plaintexts, 2^{37} memory, 2^{241} steps, (256, Kelsey)
  - 256 chosen plaintext encrypted with 2 keys, 2^{216} steps, (256, Kelsey)

Cryptanalysis 4

- CRYPTON
  - Weak keys, 2^{224} complexity, (Vaudenay, et. Al.)
  - S-boxes to be changed (2 to 4)
- DFC
  - Weak keys, reduce to 6 round cipher, prob. 2^{-64}, (Coppersmith)
  - Weak keys, pt=ct, prob. 2^{-128}, (Coppersmith)

TWOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Summary

- Claimed Attacks
  - LOKI97, FROG, MAGENTA, DEAL, SAFER + (256)
- Weak Keys 256-bits or less
  - DFC, CRYPTON
- So far pretty good
  - MARS (MF3), RC6 (MF2), RIJNDAEL (SP), TWOFISH (F), E2 (F), CAST 256 (MF1), SERPENT (SP), HPC (Omni)

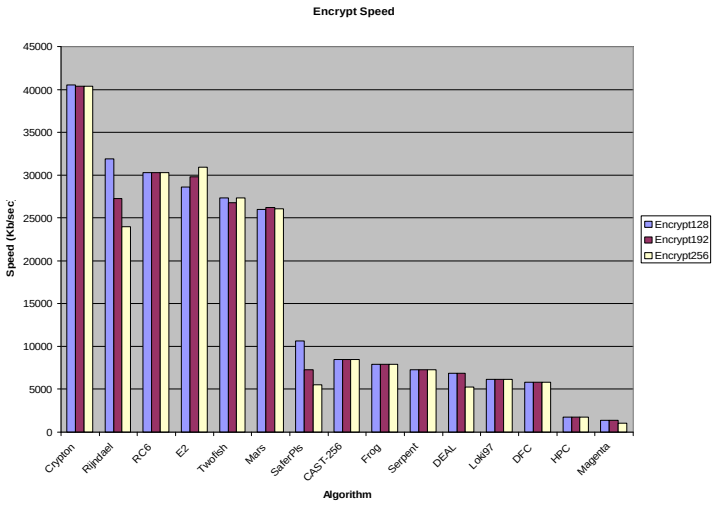
TWOFISH
SERPENT
SAFER+
RIJNDAEL
RC6
MARS
MAGENTA
LOKI97
HPC
FROG
E2
DFC
DEAL
CRYPTON
CAST-256

Cost

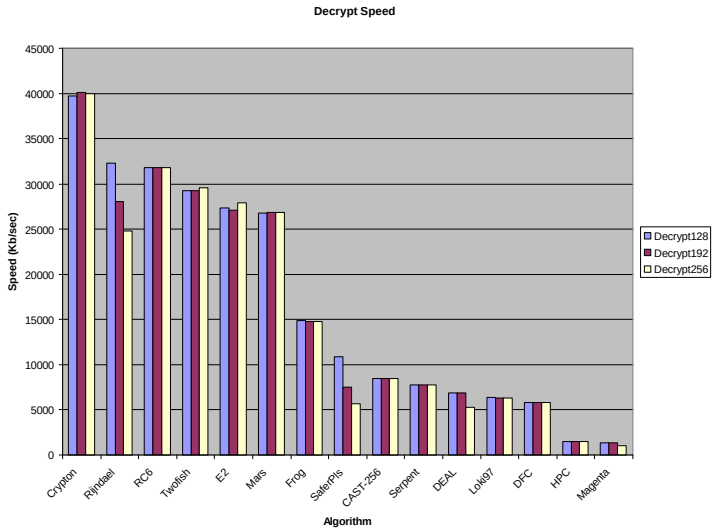
- Encryption/Decryption Times
- Key Setup Times
- Memory Requirements

NIST Platform:
IBM-compatible PC/ Intel Pentium-pro Processor 200MHz, 64MB RAM

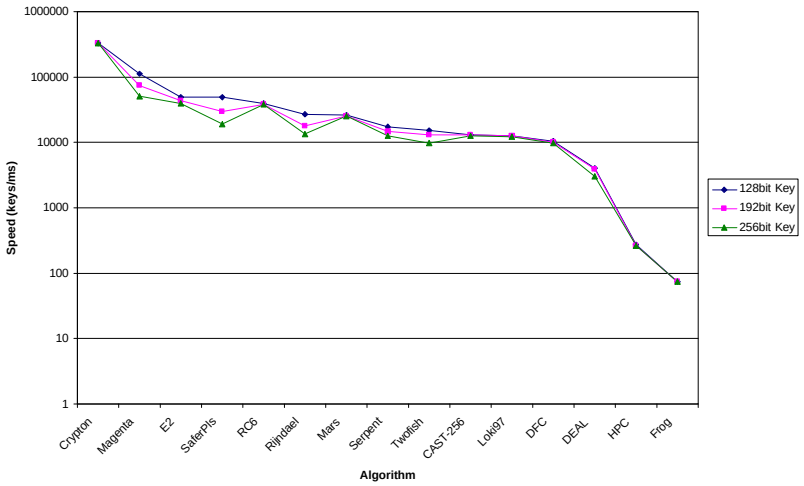
Encryption Speed on NIST Platform

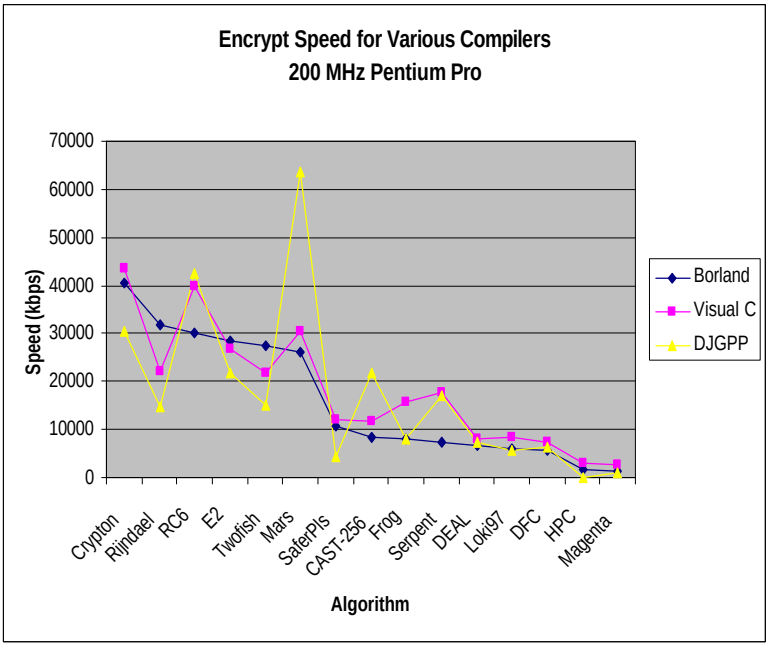


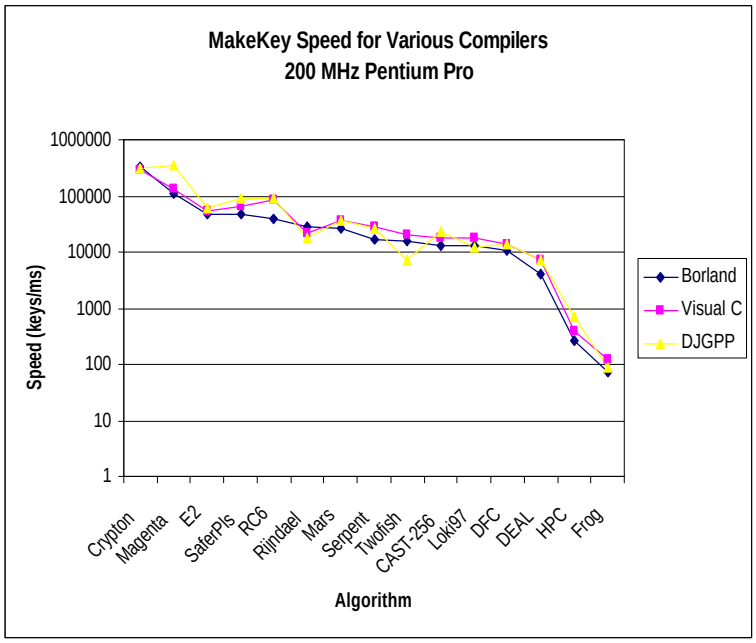
Decryption Speeds on NIST Platform



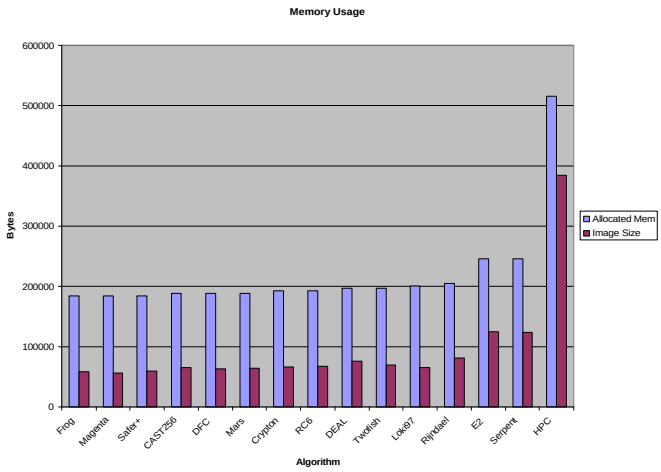
Key Set-up Speed on NIST Platform







Memory Requirements



Other Factors

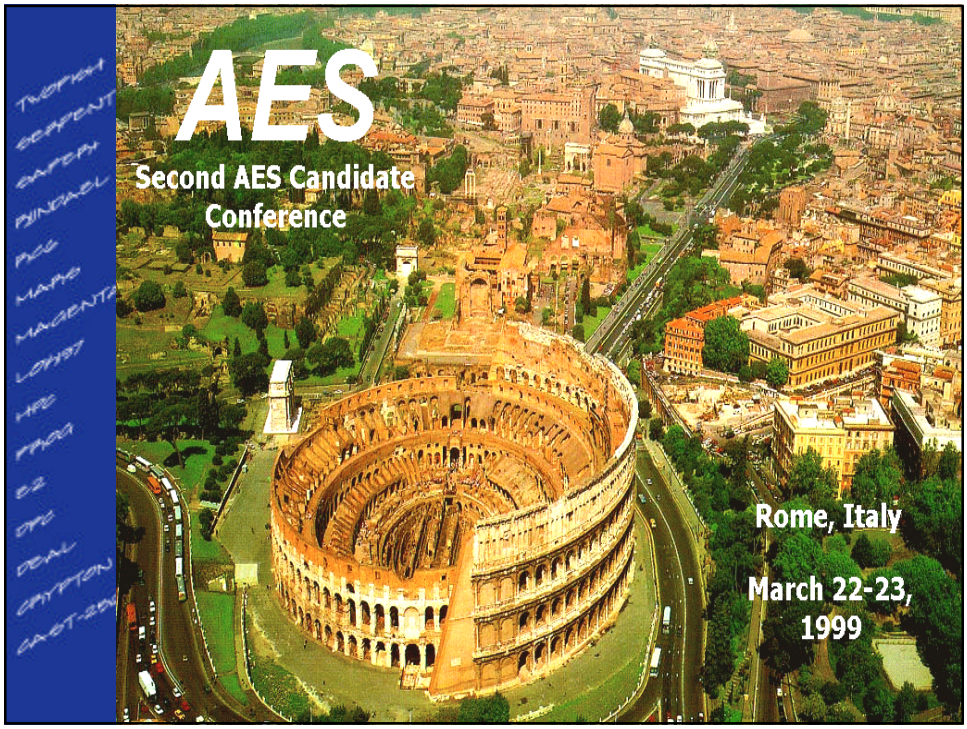
- Provable security against classes of attacks (DFC)
- Cost/Efficiency
  - Software
  - Hardware
- Architectures 8/32/64 bits
- Intellectual Property

Next Steps

- Public review of candidates, Aug. 20 - April 15, 1999
- Submissions of analysis for AES2, Feb 1, 1999
- Second AES conference, March 22-23, 1999
- Formal submissions of analysis for Round 1, April 15, 1999
- Announcement of (about) five finalists, Fall 1999
- Public Review of finalists, 6-9 months
- Third AES Conference
- Selection of AES Algorithm, 2000
- Making AES a FIPS, 2001

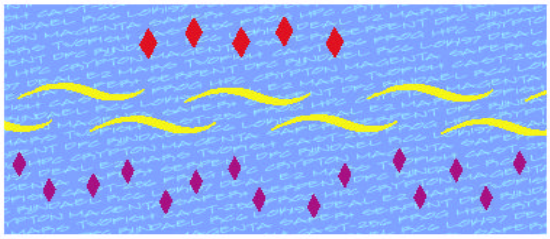
Formal Comments Requested

- How well algorithms meet criteria
  - Security, Cost, and Implementation Characteristics
- Any related intellectual property
- Cross-cutting analysis of multiple algorithms
- Overall recommendations and rationale
- e-mail: AESFIRST ROUND@nist.gov



AES

A Crypto Algorithm for the Twenty-first Century . . .



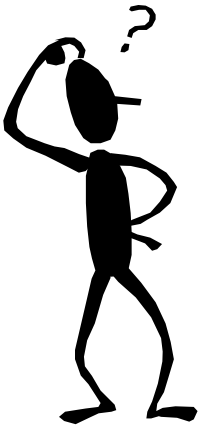
THE SECOND
ADVANCED ENCRYPTION STANDARD
CANDIDATE CONFERENCE

MARCH 22-23, 1999

HOTEL QUIRINALE
ROME, ITALY

SPONSORED BY:
INFORMATION TECHNOLOGY LABORATORY
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Summary of AES Process

- Anyone can test candidate algorithms
- Anyone can evaluate candidates
- This process requires PUBLIC participation
- To follow what is going on with AES, visit http://www.nist.gov/aes

Questions